Appendix D

Sybase Version 11.0 Test Report

Topic: Database Management System

Subtopic: Database Utilities

Test Objective 294 Verify that application provided utilities are configured appropriately and are run on a regular basis.

DII COE SRS Requirement: None Identified

Rationale: Restricts access to database and maintains security.

#	Required Action	Expected Results	Comments	Ö
1	Run the Database Consistency Check (dbcc): dbcc checktable (<tablename>) dbcc checkdb (<database name>) dbcc checkalloc (<database name>) dbcc checkcatalog (<database name>)	No problems should be found.	This utility checks the logical and physical consistency of a database.	

Topic: Database Management System

Subtopic: Recovery Management

Test Objective 292 Restore database from a previous backup and verify that data is accurate.

DII COE SRS Requirement: None Identified

Rationale: If data in the database is accidentally deleted or altered, or if a database crash occurs, the backup procedures permit the recovery of that database to a state before the problem occurred.

#	Required Action	Expected Results	Comments	Ô
1	Execute the following isql commands: select count(*) from <table_name> dump database <db_name> to dump1 where dump1 is the device name and table_name is the database table being used. truncate table table_name	Number of rows for table_name are displayed Database db_name is dumped into device named dump1. All rows in table_name are deleted.	Perform regular backups. In single-user mode, users cannot make changes until the last transaction has been restored from the dump file.	
2	Execute the following isql command: load database<db_name> from dump1 select count(*) from <table name>	Database db_name is restored from device named dump1. Number of rows for table_name are displayed. It should be the same as above.	Perform regular backups. In single-user mode, users cannot make changes until the last transaction has been restored from the dump file.	

Topic: Database Management System

Subtopic: Vulnerability Test

Test Objective 293 Attempt to modify permission on the database system tables.

DII COE SRS Requirement: None Identified

Rationale: No one should be able to change permissions on systems tables, with the exception of privileged users.

#	Required Action	Expected Results	Comments	Ô
1	Connect to Sybase as the sa user and execute the following: grant insert, delete, update on master.sysdatabases to <user_name>	Permissions are granted for <user_name>.	Prevents updates to system tables. (If an update to a system table becomes absolutely necessary, such as creating a new system procedure, refer to the System Administration documentation for the appropriate steps.)	
2	Connect to Sybase as <user_name> and attempt to impersonate another user to change permissions of the database owner: setuser "sa"	Command fails.	Prevents updates to system tables. (If an update to a system table becomes absolutely necessary, such as creating a new system procedure, refer to the System Administration documentation for the appropriate steps.)	
3	Use the SQL Server Manager to look at permission to system tables.	Permissions did not change.	Prevents updates to system tables. (If an update to a system table becomes absolutely necessary, such as creating a new system procedure, refer to the System Administration documentation for the appropriate steps.)	

Topic: Database Management System

Subtopic: File System Security

Test Objective 205 Verify that application files, configuration files, and data files are stored on the recommended drives/devices.

DII COE SRS Requirement: None Identified

Rationale: To protect the system database since it contains all system data, to protect the audit database, and to separate the software and the data files.

#	Required Action	Expected Results	Comments	Ô
1	At the Sybase server system, execute the Unix command: df	System will display directories used for the non raw partitions.	Logs should be assigned to separate devices to protect the system and audit databases when the system crashes.	
2	From isql, execute the following command: select name, phyname, mirrorname from sysdevices	Information is provided on the different devices (e.g., master, tapedump, other) and the locations where they reside. All system databases are stored on the master device. The sybsecurity database (audit) is stored on its own device. Logs are maintained on a separate device.	The Sybase executables and configuration files should not be stored in the same directory path as the data files. Logs should be assigned to separate devices to protect the system and audit databases when the system crashes. Logs can be assigned to specific devices using the "log on" clause of the "create database" command.	
3	For the different locations where the database devices reside, and for the locations where the database application programs reside, execute: ls -last <location>	System tables and data tables reside at different locations. Sybase data and sybase programs reside at different locations.	Logs should be assigned to separate devices to protect the system and audit databases when the system crashes.	

Topic: Database Management System

Subtopic: Ownerships & Permissions

Test Objective 207 Verify the application directory is owned by the proper user and the file permissions are set correctly.

DII COE SRS Requirement: None Identified

Rationale: Limits access to application files. The owner of the database application controls all reads and writes for all database transactions.

#	Required Action	Expected Results	Comments	Ô
1	Type the following command: ls -last $SYBASE	The user Sybase should be the owner of the $SYBASE directory.		
2	Execute the following UNIX command for all Sybase owned directories: ls -last<directory>	Only the user "sybase" has read and write privileges to all files in the listed directories.	Only the Sybase account has update permissions to the control files.	

Topic: Database Management System

Subtopic: Database User Groups

Test Objective 208 Verify that a group has been defined for database users and that only authorized users are members of this group.

DII COE SRS Requirement: None Identified

Rationale: Using groups limits database access to database users only.

#	Required Action	Expected Results	Comments	Ô
1	Review the /etc/group file: cat /etc/group	A group should exist for sybase users. Members belonging to the sybase group are authorized to perform administrative activities. To support separation of roles, according to the sybase installation guide, the sybase account must NOT be a member of this group.		
2	In Sybase, display existing user groups for user database(s) by executing: use<user_database> sp helpgroup	The groups for the selected database are displayed. One of the groups should identify the end users.		

Topic: Database Management System

Subtopic: File System Security

Test Objective 209 Verify that all database application files have the correct group permissions.

DII COE SRS Requirement: None Identified

Rationale: Restricts access to the application files.

#	Required Action	Expected Results	Comments	Ö
1	Type the following command: #ls -la on $SYBASE.	The permissions should be read/execute for group. The Sybase group has only read/execute permissions to all files under the $SYBASE directory.	Only the Sybase account has update permissions to the control files. This group should only have read/execute permissions to all files under the $SYBASE directory.	

Topic: Database Management System

Subtopic: Passwords

Test Objective 210 Verify that NULL passwords are not used for database level logins.

DII COE SRS Requirement: None Identified

Rationale: Having a password provides extra protection and user authentication.

#	Required Action	Expected Results	Comments	Ø
1	Use the following command to look at the master syslogins table in the master database: isql> select name, password from master..syslogins	The column Password has encrypted values for passwords.	Having a password provides extra protection from unauthorized access to database.	

Topic: Database Management System

Subtopic: I & A

Test Objective 211 Verify that database client password encryption is configured and enabled.

DII COE SRS Requirement: None Identified

Rationale: Having an encrypted password from the client provides extra protection over the network.

#	Required Action	Expected Results	Comments	Ô
1	Login to the server from a client. Then, execute an application that accesses the database. Capture the password used to connect to the database.	The password used is unreadable at the server location. Print the unreadable password.	Encrypts password before it is sent over the network.	
2	Get the encrypted password for the remote user: select name, password from master..syslogins where name="client_user_name"	The password is unreadable, and different than the password sent by the client.	Encrypts password before it is sent over the network.	

Topic: Database Management System

Subtopic: Remote Connectivity

Test Objective 224 Verify that a single remote login account to the database application is not used for multiple remote users.

DII COE SRS Requirement: None Identified

Rationale: It reduces individual accountability on the server. Audit actions can be traced only to the local server login.

#	Required Action	Expected Results	Comments	Ô
1	Login to system, and execute an application that accesses the database. Move to another terminal, and login again as the same user.	Second login connect fails. Audit log shows the failed attempt.	Audit actions can be traced only to the local server login.	

Topic: Database Management System

Subtopic: Access Control

Test Objective 212 Verify that permissions on the database system tables have not been modified.

DII COE SRS Requirement: None Identified

Rationale: Restricts access to the database.

#	Required Action	Expected Results	Comments	Ô
1	Display all sybase system tables by executing: use master sp help	All system tables in the master database are listed.	Restrict access to the system administrator account.	
2	Use the SQL Server Manager to look at permissions on all of the system tables.	Certain permissions are granted to system users but not to end users.	Restrict access to the system administrator account.	

Topic: Database Management System

Subtopic: Access Control

Test Objective 219 Verify that default passwords have been changed on any installation application login accounts or the login accounts have been deleted or locked after installation.

DII COE SRS Requirement: None Identified

Rationale: Restricts access to the database.

#	Required Action	Expected Results	Comments	Ô
1	Try logging into the "sa" account with a null password.	Login should fail.	When the server is installed, a single login called "sa", with a NULL password, is automatically configured with the SA and SSO roles. Note: For DII COE, the "sa" account is installed with a default password specified in the release notes.	
2	Login using an account with the "sa " role. Check in the "master..syssrvroles" table to verify the SSO and SA roles do not have the same user id. isql> select syslogins.suid, syslogins.name from syslogins, syssrvroles, sysloginrole where syslogins.suid= sysloginroles.suid and sysloginroles.suid=syssrvroles.suid	The SSO and SA roles do not have the same userid.	The "sa" account has all privileges of the SA role and the SSO role.	
3	Login to the "sa" account.	Login should fail.	Access to the "sa" account means unlimited access to the SQL Server. If the "sa" account is locked, check all the scripts that may contain the "sa" login name and password. Change the logins to the name of the user with the correct role. Do not lock the "sa" account until individual users with the SA_role and SSO_role have been configured correctly and	

			checked.	

Topic: Database Management System

Subtopic: Access Control

Test Objective 213 Verify that no users have the default database set to the master database.

DII COE SRS Requirement: None Identified

Rationale: Restricts access to system data.

#	Required Action	Expected Results	Comments	Ø
1	Use the following command to look in the master syslogins table: isql>select name, dbname from master..syslogins OR use the system procedure "sp_helpuser". This command gives the id in the database, group, login name, and default database.	Verify that the column for the default database for a general user is not set to master database.	Otherwise the default database is the master database.	

Topic: Database Management System

Subtopic: Access Control

Test Objective 214 Determine if separation of user roles (e.g., SSO or SA) is enforced, and if so, ensure that different individuals have been assigned to these roles.

DII COE SRS Requirement: None Identified

Rationale: Role separation is an enhanced-security feature designed to provide checks and balances to administrative responsibilities.

#	Required Action	Expected Results	Comments	Ô
1	Use the following command to look in the master..sysloginroles table to check that no two roles are assigned to same user id. isql>select suid, srid from master..sysloginroles OR isql> select syslogins.suid, syslogins.name from syslogins, syssrvroles, sysloginrole where syslogins.suid= sysloginroles.suid and sysloginroles.suid=syssrvroles.suid	Assign the SSO role, the SA role, and the Operator role to different individuals, if possible. No two rows should have the same values for column suid in the table master..sysloginroles.	Enforces and maintains individual accountability.	
2	At the Sybase prompt, type the following command: sp helpprotect	This command will display a list of all access privileges defined for all database users.	This information should show the existing controls used to restrict access of information. Not all database information should be available to all users.	
3	Look in the master..syssrvroles to check if an Application Administrator role was created. isql>select srid, name from master..syssrvroles	Create an Application Administrator role for databases that are accessed by more than one application.	Ensures proper administration of database resources. The Application Administrators may be given the privileges necessary for installing and maintaining databases accessed by the application. Having a separate database owner for the shared database provides individual accountability.	

#	Required Action	Expected Results	Comments	Ô
4	Look in the master..sysprotects table to see that the create database permission has not been granted to anyone except the system administrator. isql>select uid, protecttype, grantor from master..sysprotects where action=203	Only the system administrator has the privileges to create databases. The action value 203 corresponds to the create database command. If the protecttype value is 0, it means the permission has been granted with a "grant with grant" option. There should not exist two users having this permission.	Ensures proper administration of database system resources. The system administrator changes the ownership of the database following database creation to the appropriate Sybase user. The system procedure "sp_helprotect" is useful in listing permissions on database objects. This procedure can be used extensively for all objects, or for a specific object. If the "grantable" column is TRUE it means that the permission has been granted with the "Grant" option. For example, the command “sp_helprotect sso_role" lists all the permissions granted to the SSO role.	

Topic: Database Management System

Subtopic: Access Control

Test Objective 215 Verify that permissions for privileged roles have not been modified from the database application defaults.

DII COE SRS Requirement: None Identified

Rationale: Restricts access to the database.

#	Required Action	Expected Results	Comments	Ô
1	Look in the master..sysprotects table to see that SSO has not been granted too many permissions.	SSOs should only be given permissions to access objects that are absolutely necessary to perform SSO functions.	Examples of SSO functions are managing login accounts and the audit database.	

Topic: Database Management System

Subtopic: Access Control

Test Objective 216 Verify that no database users are given the "grant with grant option" permission to database objects. If necessary, verify any users that have this permission are valid privileged database users.

DII COE SRS Requirement: None Identified

Rationale: To restrict the transmittal of access to database objects.

#	Required Action	Expected Results	Comments	Ô
1	Look in the master..sysprotects table to see that "grant with grant" option is not used. select * from master.sysprotects where protecttype=0	No rows are returned for the query. The column protecttype does not have a value 0 which corresponds to "grant with grant".	To restrict the transmittal of access to database objects do not allow "grant with grant" option.	

Topic: Database Management System

Subtopic: Access Control

Test Objective 217 Verify that guest application login accounts do not exist. Also verify that access to database objects is not granted to PUBLIC users.

DII COE SRS Requirement: None Identified

Rationale: Prevents public access to the database objects.

#	Required Action	Expected Results	Comments	Ô
1	Look in the master..sysusers table to verify a guest account does not exist. isql>select * from master..sysusers	There should be no user with suid -1 and uid 2 which corresponds to a guest account.	To prevent public access to the database objects do not create a "guest" user account. For guest account the suid is -1 and uid is 2 and for public suid is -2 and uid is 0.	
2	Look at the master..sysprotects table to verify that permissions have not been granted to "public" on application tables. isql>select uid, action protecttype from master..sysprotects	There should be no permissions granted to user with uid 0 which corresponds to user "public."	To prevent public access to the database objects do not create a "guest" user account. For guest account the suid is -1 and uid is 2 and for public suid is -2 and uid is 0.	

Topic: Database Management System

Subtopic: Access Control

Test Objective 218 Verify that an alias mechanism is not used to treat two or more users as the same user within the database application.

DII COE SRS Requirement: None Identified

Rationale: Maintains individual traceability. To enforce security and accountability, no aliases are allowed.

#	Required Action	Expected Results	Comments	Ô
1	Look in the master..sysalternates to verify that alias have not been created. isql>select * from master..sysalternates		Using the alias mechanism prevents individual accountability for actions performed while using an alias.	
2	Execute the following sybase system procedure to see if aliases exist for database users: sp_helpuser sp_helpuser dbo	All user names for selected database are listed, but no names appear under "Users aliased to User." Get the list of all users. Get the list of dbo users.	Using the alias mechanism prevents individual accountability for actions performed while using an alias.	

Topic: Database Management System

Subtopic: Access Control

Test Objective 220 Verify that configurations variables have been set appropriately to prevent updates to the database system tables.

DII COE SRS Requirement: None Identified

Rationale: Restricts access to the database.

#	Required Action	Expected Results	Comments	Ô
1	Check in the master..syscurconfigs table to see that the value has not been modified against the default value which exists in the master..sysconfigures table.	Verify that the value has not been modified against the default values which exist in the master..sysconfigures table. By default, it is set to OFF. Do not change the configuration.	Prevents updates to system tables. (If an update to a system table becomes absolutely necessary, such as creating a new system procedure, refer to the System Administration documentation for the appropriate steps.)	

Topic: Database Management System

Subtopic: Access Control

Test Objective 221 Verify that stored procedures and triggers do not inadvertently accelerate general user permissions.

DII COE SRS Requirement: None Identified

Rationale: Permission to execute a stored procedure or a trigger gives a user indirect access to underlying database objects.

#	Required Action	Expected Results	Comments	Ô
1	The system table sysdepends contains information on references between procedures and triggers. It can be used to determine the indirect access a user may get by having access to the procedure or trigger. isql>select * from sysdepends		The system table sysdepends contains information on references between procedures and triggers. It can be used to determine the indirect access a user may get by having access to the procedure or trigger. The user inherits access privileges of the creator of the stored procedure or the trigger. Therefore, permission to execute a stored procedure or a trigger gives a user indirect access to underlying database objects.	

Topic: Database Management System

Subtopic: Audit

Test Objective 222 Verify that application level audits are generated for the vendor recommended events.

DII COE SRS Requirement: None Identified

Rationale: Ensures traceability of user actions.

#	Required Action	Expected Results	Comments	Ô
1	Check in the sybsecurity..sysauditoptions table of the audit database to see if audit options have been turned on or not. The sybsecurity..sybaudits table contains the audit records. The value of column optn (option) to enable or disable auditing is set to 1. The default value is 0 or "off."	Verify if audit options have been turned on (should not be 0 or off). The sybsecurity..sysaudits table contains audit records.	Audit to ensure that the application asks for the correct role to be turned on for a user of a specific application. Monitors remote accesses. Privileged roles such as SSO, SA, Operator, and DBO have extra permissions on database objects. To monitor the actions being performed on the objects within the database and the propagation of access permissions on these objects. Auditing the use command on the database helps in monitoring users accessing a database. To monitor the relationships between the databases and the accesses made using these relationships. Using the setuser command a user can take on the identity of another database user. This can subvert individual accountability for actions performed by a user.	

Topic: Database Management System

Subtopic: Recovery Management

Test Objective 225 Verify that backups of the database can be performed and that they are performed on a regular basis.

DII COE SRS Requirement: None Identified

Rationale: Ensures recovery from failures.

#	Required Action	Expected Results	Comments	Ô
1	Check in the audit trail to determine if backups are made. The database audit trail is stored in the sybsecurity..sysaudits table.	Frequent backups of the database have been made.	Backups may be performed using the "dump database" and dump transaction" commands. The database is locked using the "set_dboption" to set the "no chkpt on recovery", "dbo use only", and "read only" options to TRUE. Configuration of a Backup Server is discussed in detail in the Systems Administration Guide. Use single user mode when reloading from the backup created by the dump database command.	

Topic: Database Management System

Subtopic: Recovery Management

Test Objective 248 Verify that important database configuration files and logs are being mirrored.

DII COE SRS Requirement: None Identified

Rationale: Ensures recovery from failures.

#	Required Action	Expected Results	Comments	Ô
1	Disk mirroring for rapid recovery may be used. Inspect code used for the sybase database creation.	Disk mirroring was used.	The master device, user databases, and the transaction log are all stored on different partitions of the same physical device, and are all mirrored to a second physical device. Failure of either disk will not interrupt SQL Server users. The drawback is that applications with a lot of update transactions may be slower. There are other options for mirroring based on cost and performance trade-offs.	
2	From isql, execute the following command: select name, phyname, mirrorname from master.sysdevices	Information is provided on the different devices (e.g., master, tapedump, other) and the locations where they reside. Check for mirrored devices.	The master device, user databases, and the transaction log are all stored on different partitions of the same physical device, and are all mirrored to a second physical device. Failure of either disk will not interrupt SQL Server users. The drawback is that applications with a lot of update transactions may be slower. There are other options for mirroring based on cost and performance trade-offs.	

Topic: Database Management System

Subtopic: Audit

Test Objective 226 Verify that any database auditing features, if they exist, are configured and operational. Verify that only authorized users can modify database audit features.

DII COE SRS Requirement: None Identified

Rationale: An audit trail for database transactions is needed to identify problem areas, as well as identify any attempts made to circumvent security mechanisms.

#	Required Action	Expected Results	Comments	Ø
1	Use the following command to determine if the "sysecurity" database exists. use sybsecurity sp help	If the "sybsecurity" database exists, no error messages will be displayed.		
2	Connect to the database as a privileged user and turn off audit option: sp audit option Look at audit options after the change: select * from sysauditoptions Connect as the privileged user again and turn on the audit option: sp audit option Connect to the database as a non-privileged user and attempt to turn off the audit option: sp audit option	The final command will fail. Information should be captured in audit logs.		
3	Review the audit logs: select * from sybsecurity..sysaudit where <date expression>	Depending on the conditions substituted in the where clause, a day's worth of audit data will be displayed.		